

Xinyi Liu. Design and Development of a Web-based Platform to Manage Information Resources Security in Higher Education. A Master's Paper for the M.S. in IS degree. April, 2018. 54 pages. Advisor: Arcot Rajasekar

This paper describes the design and development of a web-based platform to assess, analyze, and manage information resources security in higher education. The paper studies the types of assets, threats, and vulnerabilities that are used and faced by higher education and how-to categorize them into different security levels. The platform manages information resources by creating and operating independent security projects. It takes the user's input of asset, threat, and vulnerability information of each project as attributes and saves the data to a back-end database, then follows risk assessment metrics to calculate and determine risk value and level. Additionally, the visualization module provides the user a cross-view of all existing security projects based on the type and number of the asset, threat, and vulnerability to further assess and analyze them based on visual analytics.

Headings:

Information Resources Security

Web Design and Development

Risk Assessment

Information Visualization

DESIGN AND DEVELOPMENT OF A WEB-BASED PLATFORM TO MANAGE
INFORMATION RESOURCES SECURITY IN HIGHER EDUCATION

by
Xinyi Liu

A Master's paper submitted to the faculty
of the School of Information and Library Science
of the University of North Carolina at Chapel Hill
in partial fulfillment of the requirements
for the degree of Master of Science in
Information Science.

Chapel Hill, North Carolina

April 2018

Approved by

Arcot Rajasekar

Table of Contents

1	INTRODUCTION.....	2
1.1	MOTIVATION.....	2
1.2	OBJECTIVE.....	3
1.3	RESEARCH QUESTIONS	4
2	PRIOR WORK.....	6
2.1	INFORMATION RESOURCES IN HIGHER EDUCATION	6
2.2	THREAT & CHALLENGES	7
2.3	RISK ASSESSMENT	9
2.3.1	<i>Asset categorization and value definition</i>	<i>9</i>
2.3.2	<i>Risk Management vs. Risk Assessment.....</i>	<i>10</i>
2.3.3	<i>Controls.....</i>	<i>11</i>
2.4	INFORMATION SECURITY VISUALIZATION.....	13
2.4.1	<i>What is Security Data Visualization?.....</i>	<i>13</i>
2.4.2	<i>Type of Security Data Visualization Tools.....</i>	<i>13</i>
3	DESIGN OF THE INFORMATION RESOURCES SECURITY MANAGEMENT PLATFORM IN HIGHER EDUCATION.....	16
3.1	SYSTEM ARCHITECTURE DESIGN.....	17
3.1.1	<i>Module Design.....</i>	<i>17</i>
3.1.2	<i>Use Case View.....</i>	<i>19</i>
3.1.3	<i>Process View.....</i>	<i>20</i>
3.1.4	<i>Database Schema Design.....</i>	<i>22</i>
3.2	USER INTERFACE DESIGN.....	23
3.3	RISK ASSESSMENT METRICS	26
4	EVALUATION OF THE INFORMATION RESOURCES SECURITY MANAGEMENT PLATFORM IN HIGHER EDUCATION.....	30
5	CONCLUSION	33
	 APPENDIX A: DEVELOPMENT OF THE INFORMATION RESOURCES SECURITY MANAGEMENT PLATFORM IN HIGHER EDUCATION.....	 40
I.	DEVELOPING AND OPERATING ENVIRONMENT	40
II.	IMPLEMENTATION OF THE DATABASE	40
III.	IMPLEMENTATION OF THE PLATFORM.....	42
1.	<i>Implementation of Project Management.....</i>	<i>42</i>
2.	<i>Implementation of Asset Management</i>	<i>43</i>
3.	<i>Implementation of Threat Management.....</i>	<i>45</i>
4.	<i>Implementation of Vulnerability Management.....</i>	<i>47</i>
5.	<i>Implementation of Control Management</i>	<i>49</i>
6.	<i>Implementation of Risk Assessment</i>	<i>50</i>
7.	<i>Implementation of Visualization</i>	<i>51</i>

1 Introduction

1.1 Motivation

Higher education in the U.S is highly digitalized today due to the development of the Internet and information technology. Various systems are in place to support students' education, faculty members' teaching, and staffs' working needs. Almost every school has its own website working as a window or platform to present school information on Academics, Research, and Programs, which is a useful and must-have channel for the propagation of the school and its information. There are numerous internal and external access points to all websites and sub-websites. In both use cases, system and website, different types of data are generated, so further security needs are raised such as data transaction, data storage, data exchange, and data access. It is obvious that all the information resources in schools have a great number of users, if any part of the system gets broken and stops working, it will have great effects on system performance, users experience, research projects, school reputation, or management of education, which means the security and integrity of all the information resources in an education organization are very important.

Because of the huge volume of information resources in higher education, various types of information security incidents have happened in recent years. Researchers from the Digital Citizens Alliance (Cortez, 2017) found almost 14 million email addresses and passwords from faculty, staff, students and alumni at U.S. universities. About 79 percent of the credentials were put on the dark web in the year of 2016 alone. The problem is ongoing.

Illegal access to web-based information systems and use of malware software urgently needs attention.

At the current stage, most higher education facilities have firewalls configured, anti-virus software installed, and the framework follows certain Information Security standards. However, the effectiveness of protecting information resources and managing security risks and controls needs to be improved. Additionally, the metrics and approach to manage information resource security are relatively isolated and inconsistent, there is lack of a unified and collaborative platform for all information security officers to manage IT security related projects. In order to build up a feasible and effective security protection system, risk assessment is very beneficial to evaluating and offering better controls for the security of all information resources. Data visualization is another critical technique to further represent, analyze, and predict based on data.

1.2 Objective

The goal of this project is to research the potential security threats to information resources in education organizations, study how risk assessment will benefit understanding and prevention of information security incidents, integrate data visualization to support Information Security Staff to analyze the risks and controls based on visual presentations, then design and develop a web-based platform to analyze, assess, and manage information resources security in education organizations.

Objectives breakdown: 1) information resources in higher education includes all kinds of data, with this platform users will be able to categorize information based on the resource type; 2) existing management approaches rely on human being's cognition and past experience, which is inconsistent and nontransferable when it comes to collaboration, this platform will

record and digitize the information to further support describing assets, threats, and risks; 3) the management of IT resources and security related projects in higher education are relatively focused on individual components rather than the overall effect or the relation between components, instead, each project in this platform will have an overall risk assessment based on each component's risk, which can also be easily updated if any changes occur to the project; 4) various types of information and data are generated when using the platform to manage information resources from a security perspective. It is hard to generate meaning based on a table representation of the input data. This platform integrates visualization components to provide the users a clearer and more comprehensive approach to analyze the data and better understand the risks and controls.

1.3 Research Questions

RQ1: What types of information resources and associated security threats are there in higher education?

This part of the research will include the overview and knowledge of information resources in higher education and lists of potential threats to each one of the resources.

RQ2: How to assess the risk of information resources in higher education?

This part of the research will include the definition of general risk assessment and what it should be in the environment and settings of higher education, which will include model design, process design, asset categorization, vulnerability categorization, threat categorization, and the metrics used to compute the value of the level of risk.

RQ3: What types of security visualization technologies are available in higher education?

This part of the research will include currently available security visualization technologies, and further expand on which concepts can be integrated into this platform. The

visualization in this project will be focusing on presenting the data that is manually input by the users and providing analytic function for the users.

RQ4: How is the web-based platform to analyze, assess, and manage information resources security in education organizations designed and developed?

This part of the research will focus on the design and development of the platform, which includes framework, database, interface, and interaction. Last but not least, the performance of the completed system when performing different tasks will be tested.

The following chapters will provide a detailed introduction and description of what research has been done and the design & development processes of the project. Chapter 2 introduces previous research and work on information resources security management, what risk assessment methods are available and what visualization tools are in place. Chapter 3 focuses on the design process and details of the web-based information resources security management tool. Chapter 4 is about testing and evaluation of the management platform to see if there is potential enhancement based on the current implementations. Chapter 5 is the conclusion of the paper which provides answers to the initial research questions, lessons learned and future improvement of the developed product. In Appendix A, it shows the outcome of the project that includes all the development and implementation details.

2 Prior Work

This Chapter describes and concludes prior research work that is helpful to the design and development of my work. All the studies in this chapter not only gives me the chance to learn about the current state of the research areas but provides me ideas and supportive materials to my own study. It includes all the key concepts: information resources in higher education, threats, risk assessment, and information security visualization.

2.1 Information Resources in Higher Education

The object of this project is information resources in higher education, which may refer to 1) A **system resource** in computer science; any component of limited availability within a computer system; 2) A **web resource**; a data source accessible on the World Wide Web; 3) An **electronic resource**, information which can be stored in the form of electrical signals.

The Columbia University Information Security Charter (2016) defines information resources in the scope of Information Security Policies as: 1) All Data regardless of the storage medium (e.g., paper, fiche, electronic tape, cartridge, disk, CD, DVD, external drive, copier hard drive, etc.) and regardless of form (e.g., text, graphic, video, audio, etc.); 2) The computing hardware and software Systems that process, transmit and store Data; 3) The Networks that transport Data.

Giszcak et al. (2016, August 23)'s report on data privacy and cybersecurity in higher education categorizes information resources in higher education from a different perspective:

“From social security and credit card numbers to health care records and intellectual property produced by research departments, colleges and universities house a vast amount of sensitive data.”

The report lists various forms of data that need to be protected in higher education: 1) personal and financial information; 2) health information; 3) intellectual property; 4) government data; 5) employment-related records; 6) retail establishments.

The challenge of categorizing information resources in higher education is that different schools have different types of resources and they organize them in different ways. How to include them all while not overwhelming the users is a critical problem to be solved while making design decisions.

2.2 Threat & Challenges

In Universities UK (2013)’s report on cyber security and universities, it introduces two types of threats in Table 1:

Advanced state and corporate threats	Theft of sensitive corporate data for competitive advantage Theft of sensitive corporate data	Theft or damage to valuable research and data
‘Hacktivist’ and criminal threats	Disruption of infrastructure - e.g. overloading of websites	Theft of sensitive personal data for fraud or political purposes

Table 1: Types of threats

In many countries, there are laws, regulations, and policies, governing information security, such as the Data Protection Act and Computer Misuse Act in the United Kingdom and the Federal Information Security Management Act in the United States. In Hong Kong, a set of baseline policies have been established for enforcing information security in government offices. Additionally, many national and international standards for information security

management have been established. Among these standards, the ISO 27000 Information Security Management System is the most widely adopted. ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003, ISO/IEC 27004 and ISO/IEC 27005, with related terms and definitions.

The consequences of various security incidents may have a huge impact on:

- Reputation: information theft and integrity issues may severely harm a university's reputation in the eyes of students, partners, businesses and governments.
- Legal: theft of information may leave institutions in breach of legislation or contracts and at risk of prosecution, penalties and withdrawal of existing and future funding.
- Economic: theft of information may directly undermine a university's or researcher's ability to capitalize on potential intellectual property or knowledge transfer.
- Operational: there may be immediate damage to networks and infrastructure that prevents or hinders an institution's activities and results in significant remedial costs.

Since most information systems in higher education are web-based, they face similar threats as web applications, such as 1) cross-site scripting; 2) SQL injection; 3) remote command execution; 4) directory listing ... this leads to data breach, malicious tampering, system destruction and etc. Web resources such as websites are platforms and interfaces, used to present and provide information. Thus, their stability and security are also very important. They're at risk of threats like 1) insecure website login method; 2) directory listing; 3) SQL injection; 4) deadlock and phishing ... which results in account hijacking and further financial loss. As for data, it is common to experience Advanced Persistent Threat (APT). APT is an advanced sustainability attack that is widely used by hackers to conduct long-term, fixed-target, consistent attacking. The threats for hardware are 1) lack of management or misuse by

personnel; 2) improper operation; 3) threat to the physical environment. It is a necessity to have relevant management strategies in place to minimize potential risk.

2.3 Risk Assessment

2.3.1 Asset categorization and value definition

According to Bishop (2003) and Peltier (2004)'s research, the CIA triad forms the principles of information security, which include confidentiality, integrity, and availability. In the other literature of Parker (2002) and Anderson (2003), they argued that the CIA triad should be extended to six principles. They add authenticity, non-repudiation, and accountability. Figure 1 shows these principles:

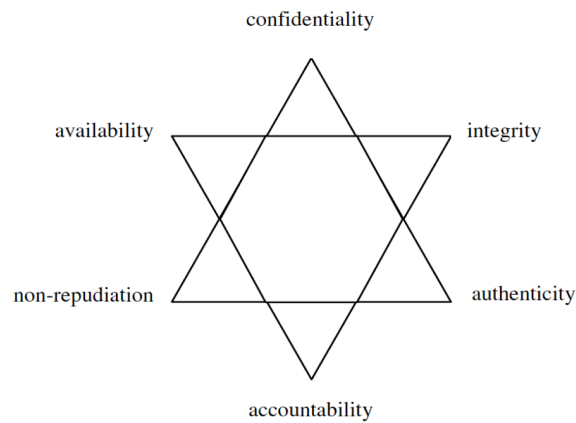


Figure 1: Six principles of Information Security

Confidentiality is the ability to protect information from unauthorized access. **Integrity** is the ability to protect information from undetected modification or deletion. **Availability** is the ability to protect information from attacks by denying or inconveniencing unauthorized accesses. It ensures that information is readily accessible to the authorized users at all times. **Authenticity** is the ability to ensure that transactions or communications of information are genuine. In order to validate accesses to information, authentication system

with proper access control and password protection is adopted. Nonrepudiation refers to one's intention to fulfill the accepted obligations. Accountability is the ability to track user identity and actions applied to the information. Accountability is a useful element for executing non-repudiation that proves the performance of an action (Cheung, 2014, p. 13).

2.3.2 Risk Management vs. Risk Assessment

“Maslow recognized risk in his famous hierarchy of needs by placing food and shelter, both essential to survival, on [sic] the first rung of the ladder” (Rao, 2009, p. 87). In his book, *Against the Gods: The Remarkable Story of Risk*, Bernstein (1998), an economist and financial historian, traces the history and evolution of “risk,” explaining that the modern concept of risk is rooted in the Hindu-Arabic numbering system and games of chance of the Greeks and Romans, noting that the concept of risk management emerges during the Renaissance with the inception of probability theory. “Risk management guides us over a vast range of decision-making, from allocating wealth to safeguarding public health, from waging war to planning a family, from paying insurance premiums to wearing a seatbelt, from planting corn to marketing cornflakes” (Bernstein, p. 2).

While risk management is a systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analyzing, evaluating, treating, monitoring and communicating risk, risk assessment involves evaluating existing security and controls, and assessing their adequacy relative to the potential threats of the organization. Instead of managing policies and procedures, risk assessment is a quantitative assessment of the possible impacts caused by a security incident, which may have already happened, be currently happening, or will happen. Information security risk assessment is the assessment of the value, threats, and vulnerabilities of information resources.

According to Trusted Computer System Evaluation Criteria (TCSEC), risks are qualitatively expressed as Critical, High, Medium, Low and Minimal. For purposes of this Policy, Critical, High, Medium, Low and Minimal Risks are defined as in Table 2:

Level of the Risk	Description of the Risk
Critical Risk	The risk of imminent compromise or loss of Sensitive Data from either external or internal sources or where Sensitive Data has already been exposed. There is no control in place to protect the Data
High Risk	The risk of imminent compromise or loss of Sensitive Data from either external or internal sources. There is only a single control, or multiple ineffective controls, in place to protect the Data
Medium Risk	The risk of compromise or loss of Sensitive Data is possible from either external or internal sources, although less likely from external sources. Controls are in place that are somewhat effective to protect the Data
Low Risk	The risk of compromise or loss of Sensitive Data is possible, but not probable or an Information Resource might be used to obtain access to Sensitive Data on a different Information Resource
Minimal Risk	There is no realistic risk of compromise or loss of Sensitive Data

Table 2: Level of Risk. Retrieve from The Trusted Computer System Evaluation Criteria (1983-1999). <https://www.cs.clemson.edu/course/cpsc420/material/Evaluation/TCSEC.pdf>

2.3.3 Controls

It is necessary for a higher education institution to establish policies and control measures for ensuring information security (Rezgui & Marks, 2008). It is challenging to apply the principles of information security to practical use. The ISO 27001 Information Security Management System provides a thorough coverage of the key control areas of information security as summarized in Table 3. By making reference to ISO 27001, there are at least eight control areas for a higher education institution, namely, information asset controls, personnel controls, physical controls, access controls, communication controls, operation controls, information system controls, and incident management and business continuity (Cheung, 2014, p. 13).

Control Area	The purpose of the policy	Action needed for Higher Education
Information Asset Controls	Policies should be established to ensure that appropriate levels of protection and	Information assets should be classified, and the owner,

	accountability are maintained for information assets. This should be made in accordance with the sensitivity, criticality and values of information assets.	custodian and users of the information assets should be well defined.
Personnel Controls	Policies should be established to ensure that everyone in an organization clearly understand his or her roles and responsibilities to reduce the risk of theft, fraud or misuse of information assets.	All staff should be aware of the information security threats and concerns and are equipped to support information security in the course of their normal work and reduce the risk of human errors.
Physical Controls	Policies should be established to ensure that appropriate physical security and control should be maintained to protect against any unauthorized accesses to some defined secure areas such as data centres.	Computer systems and storage of critical and sensitive information shall be housed in data centres with proper physical access controls.
Access Controls	Policies should be established to ensure that access control to information systems and information processing facilities, and that access rights are properly authorized, allocated and maintained. Control measures should be implemented to enforce authorized accesses to information as well as to reduce the risks of unauthorized access, loss or damage to information.	There should be proper access controls for information systems and information processing facilities, where student information and financial information are stored. An access control table should be defined for each information system.
Communication Controls	Policies should be established to define procedures for the management and operation of network and communication facilities. Control measures should be implemented to maintain the confidentiality, integrity and availability of communication facilities, such as electronic mailing systems and network storage for information exchange.	Electronic communication is very common. Electronic mails containing student information or sensitive information should be handled with care. It is a good practice to use secured electronic mail systems to protect sensitive information from undetected interception, modification or omission.
Operation Controls	Policies should be established to define procedures for the management and operation of computer systems and information processing facilities. Control measures should be implemented to maintain the confidentiality, integrity and availability of the computer systems and information processing facilities.	System fixes and patches, especially those related to information security, should be timely applied. Backup procedures should be tightly followed, and tapes and disks should be properly stored.
Information System Controls	Policies should be established to ensure proper controls to prevent information systems from any unauthorized modification and misuse of information. Information security requirements should be clearly identified at the beginning of system development.	The input, processing and output of student information should be properly defined and implemented. These should be enforced during the acquisition, development and maintenance of information systems.

Incident Management and Business Continuity	Policies should be established to ensure that information security incidents are communicated in an appropriate manner, allowing timely corrective actions to be taken.	Teaching and learning are critical, and hence, control measures should be enforced to maintain continuity of teaching and learning activities in case of information security incidents.
--	---	--

Table 3: 8 key control areas of information security (Cheung, 2014, p. 14).

2.4 Information Security Visualization

2.4.1 What is Security Data Visualization?

SANS Institute (2015)'s report on Security Data Visualization explains how security data visualization can be used in many areas of information security. Security metrics, Security monitoring, anomaly detection, forensics, and malware analysis are examples of where security data visualization can play a vital role in supporting information security professionals. Security data visualization is part of data science and requires skills in hacking, statistical knowledge and domain knowledge (SANS Institute, 2015, p. 3). The paper also introduces the process of Security Data Visualization: 1) Visualization goals; 2) Data Preparation phase; 3) Exploration phase; 4) Visualization phase; 5) Feedback and fine-tune.

2.4.2 Type of Security Data Visualization Tools

Shiravi et al. (2012) classify the recent works of network security visualization into five use-case classes. They are host/server monitoring, internal/external monitoring, port activity, attack patterns, and routing behavior. Each use case represents a different application area, were defined and several recent works in each category were thoroughly described.

- Host/Server Monitoring

In this class of visualization, the main display is devoted to the representation of hosts and servers. The intent is to display the current state of a network by visualizing the number of users, system load, status, and unusual or unexpected host or server activities. Systems of

this class should also be able to correlate communicating processes of a single host or server with the network traffic. This feature enhances the ability of a user to identify malware as they often manifest themselves in irregular and often anonymous system processes (Shiravi et al., 2012, p. 1315).

- Internal/External Monitoring

Visualizations of this class are concerned with the interaction of internal hosts with respect to external IPs. Similar to the above-mentioned class, this class of visualization also incorporates a display of internal hosts, but in relation to communicating external IPs. Since the art of displaying internal hosts in a nonoccluding and meaningful manner is by itself a delicate act, adding the burden of displaying hundreds and thousands of external IPs is a nontrivial process for systems of this class (Shiravi et al., 2012, p. 1317).

- Port Activity

Visualizations of this class can aid in the detection of malicious software running inside a network. Scaling techniques must be incorporated in the design of visualizations of this class, due to the amount of traffic as well as the large range of possible port numbers and IP addresses (Shiravi et al., 2012, p. 1318).

- Attack Patterns

Visualizations of this class aid an administrator in not only the detection of attacks but also the display of multistep attacks. Different types of attacks show different behaviors and accordingly different visual patterns appear. Many types of attacks are carried out in multiple phases, generally starting with reconnaissance, followed by scanning, acquiring access, maintaining access, and finally clearing tracks and installing back doors for future access. Visualizations of this class should aid in displaying these phases (Shiravi et al., 2012, p. 1319).

- Routing Behavior

Understanding the evolution of Border Gateway Protocol (BGP) routing patterns over time is the main goal of this visualization class. The distributed nature of BGP and the lack of verification of the validity of the announcements causes Internet routing to be susceptible to attacks. The ability to detect and correct disruptions in Internet traffic caused by router misconfigurations or malicious attacks is considered in this class (Shiravi et al., 2012, p. 1323).

3 Design of the Information Resources Security Management Platform in Higher Education

Based on the research on prior work in chapter 2, chapter 3 is about the design process of the proposed platform for managing information resources security in higher education.

The motivation of building a web-based information resources security management platform is there is no such unified and targeted platform for information resources security in higher education, while a system is needed to support specific security projects management instead of an overall and undifferentiated management platform for all types of IT projects since the features and attributes that are required to evaluate and analyze a security project are unique and more specific.

Based on the previous study and information gathering, there are major concepts/aspects that need to be included to make the platform feasible and helpful to security analysts in higher education, they are 1) asset, 2) threat, and 3) vulnerability. These three attributes together describe the key components of a security project and they provide support as well as a base for risk assessment. Moreover, data visualization is integrated into the platform to provide analysts the ability to analyze and manage the projects from a visual perspective.

The first step of implementing the proposed platform is designing, so in this chapter, it uses different models to explain and illustrate the design from different angles with various focus. Module Design separates functionalities into chunks of with specific modules that handle different sub-functions. Use Case View explains how the potential users would interact

with the platform and what functions are available to certain users with different accesses. Process View focuses on how users' action would trigger the read/write operations between the front-end and the database. Database design shows the detailed schema of the back-end database and what columns are included in all the tables. Last but not least, the UI design is presented which includes all the draft digital prototypes of major interfaces.

3.1 System Architecture Design

3.1.1 Module Design

Module Design is used to illustrate the system design from a broader and overall view without touching on detailed flows and processes. It gives a clear and organized view of what modules are included and what sub-modules are under them. There is hierarchy organization of the design since it follows the workflow of the information resources management platform.

As shown in Figure 2, the web-based information resources security management platform asks user to input project information; then based on each project, add the associated asset data; then based on asset, input the corresponding threat it faces; then according to the threat information, the vulnerability is added that represents how vulnerable and easy to hack an asset is. After three attributes' data is input, risk assessment module takes all the data and calculates associated risk. The visualization module is the module that takes all existing projects' information and shows a cross-view of the projects on asset types, threat types, and vulnerability types.

For the sub-modules, the project module includes functions: add a project, delete a project, and select project (to show the information of selected project for all pages). The asset module includes add an asset, delete an asset, view asset, and set value for the asset. The threat module includes add threat, delete threat, view threat, and set value for the threat. The

vulnerability module includes add vulnerability, delete vulnerability, view vulnerability, and set value for the vulnerability. The control module allows the user to add control, delete control, and view control. The risk assessment module handles risk calculation, and the visualization module generates visualization based on the users' former input for the asset, threat, and vulnerability modules.

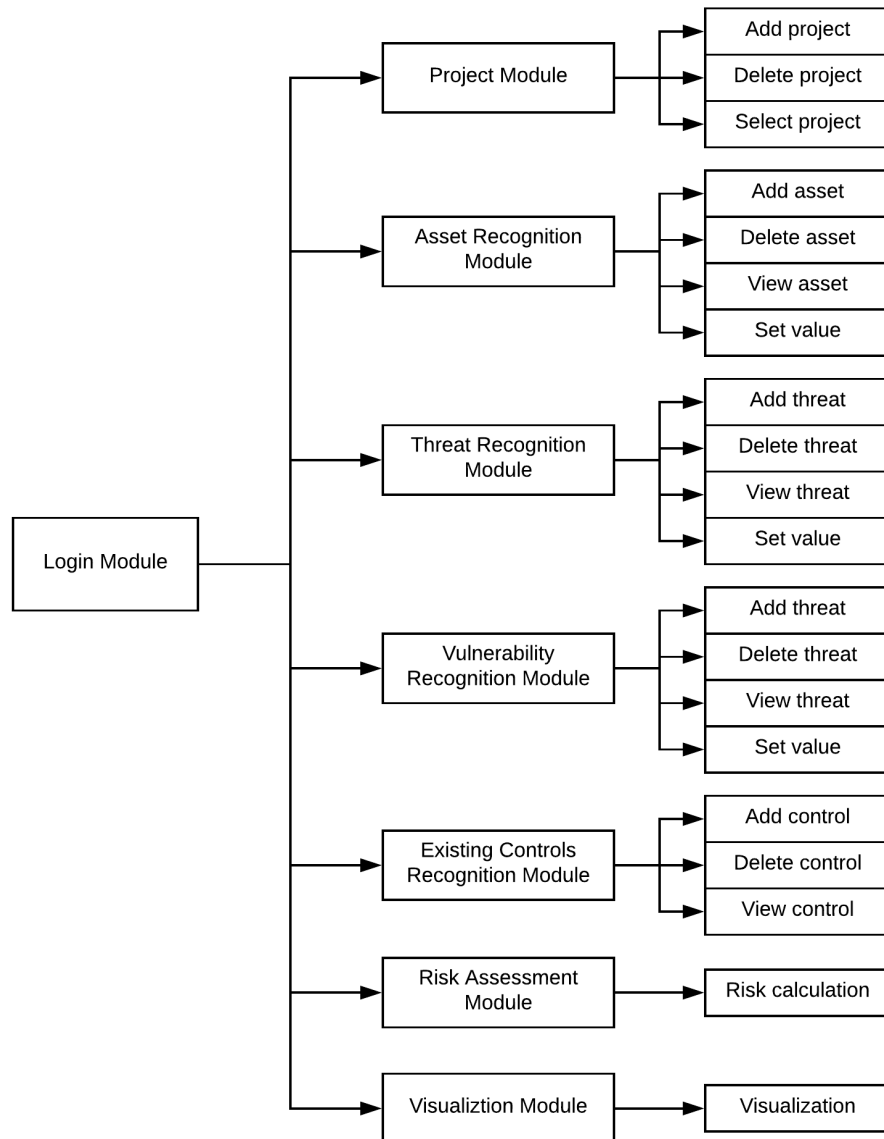


Figure 2: Information Resources Security Management Platform - module design

3.1.2 Use Case View

Use Case View is a view of system functions used by system operators. A Use Case View shows all the interactions between users and the system. The view presents what type of operation is conducted by the users. The Use Case View of the web-based information resources security management platform is shown in Figure 3:

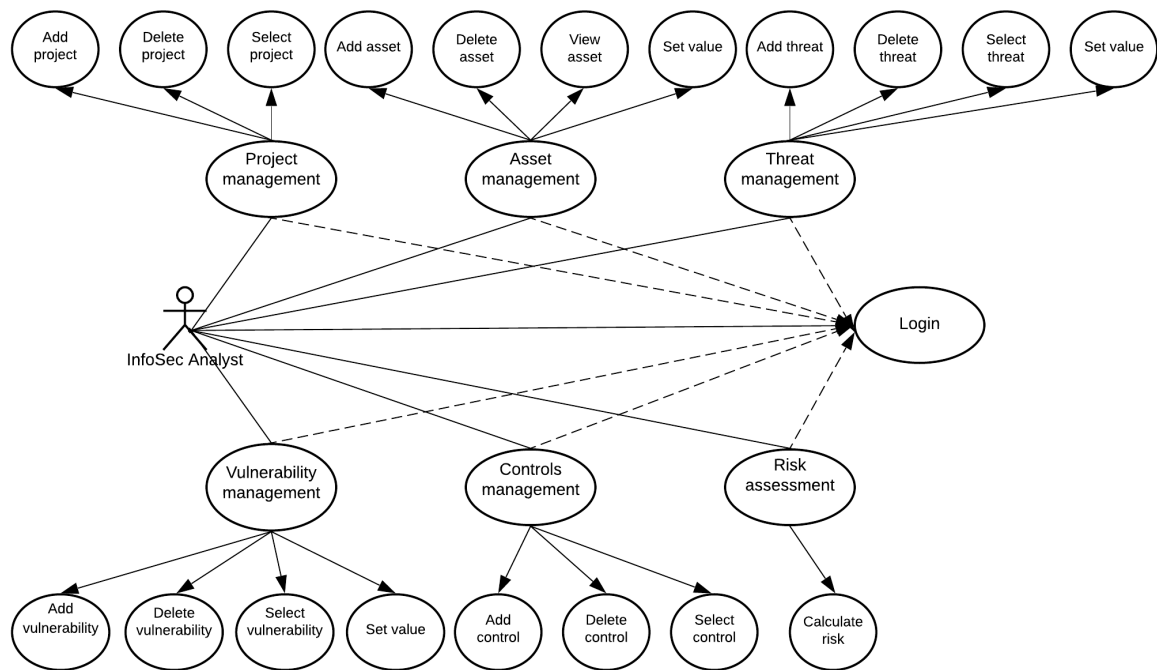


Figure 3: Information Resources Security Management Platform - Use case view

In Figure 3, the solid lines between the analyst and cases represent the functions that the analyst can use; the dotted lines between cases and the login module represent the operations that can be conducted after logging in. Detailed instruction for each use case is listed in Table 4:

Case	Instruction
Login	Analyst uses valid user name and password to log into the platform.
Project management	Analyst can add and delete project. Analyst can also select project to view and work on.

Asset management	Analyst can add, delete, view, and set value for asset.
Threat management	Analyst can add, delete, view, and set value for threat.
Vulnerability management	Analyst can add, delete, view, and set value for vulnerability.
Control management	Analyst can add, delete, and view control.
Risk assessment	Analyst can calculate the risk.

Table 4: Case Instruction

3.1.3 Process View

Use Case View describes operations that can be conducted by the analyst, which leads to the detailed process design, while Process View makes it easier to further understand the detailed processes that happen within every operation.

- **Login Operation**

This is an operation that happens when analyst tries to log into the platform, the user interacts directly with the view. When the user inputs username and password information and submits it to the back-end, the controller passes the data and queries the database to check if the data is valid. If it passes the authentication, the platform guarantees the access to further functionalities. If not, it throws an error message and denies the access request. The process is shown in Figure 4:

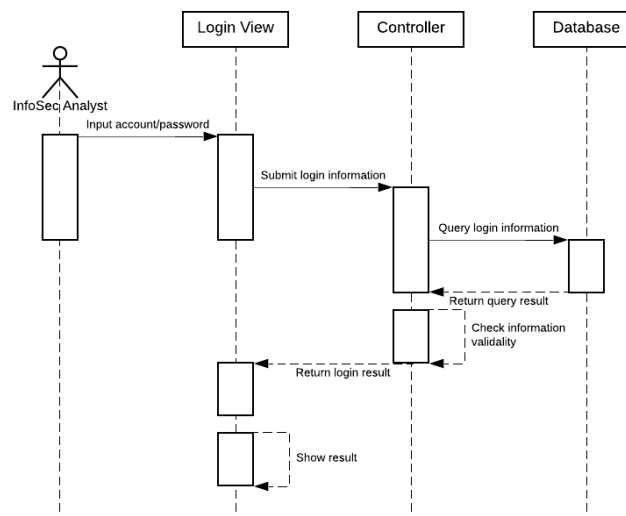


Figure 4: Login operation process view

- **Add/delete/set value Operation**

Add, delete, and set value operations follow a similar process when communicating with the database. In Figure 5, I use “Asset Management” as an example with “Add New Asset” operation, the analyst needs to input required fields on the page and click on submit, which triggers a query of inserting a row to the corresponding table in the database. The flow is the same for delete as well as set value requests, the difference is the query changes depending on the “read” and “write” actions.

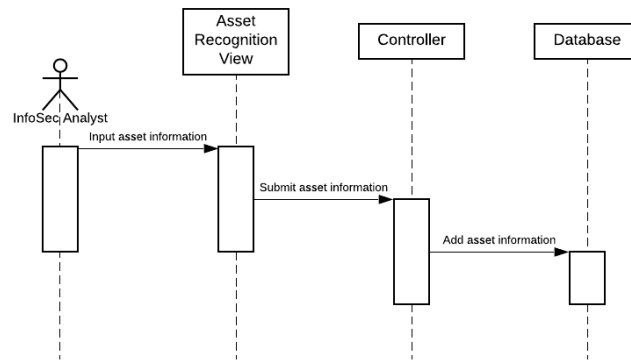


Figure 5: Add operation process view

- **View Operation**

When an analyst chooses to view existing instances, as shown in Figure 6, it uses “View Asset” as an example, the controller sends the query to request all existing assets’ information. If there is data saved in the database, then it returns all the instances, then the controller handles the data formatting and displays them in the view.

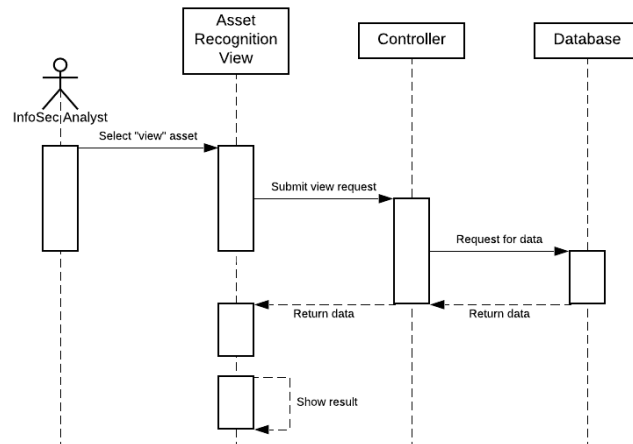


Figure 6: View operation process view

3.1.4 Database Schema Design

As shown below in Figure 7, this is the database schema design for the system:

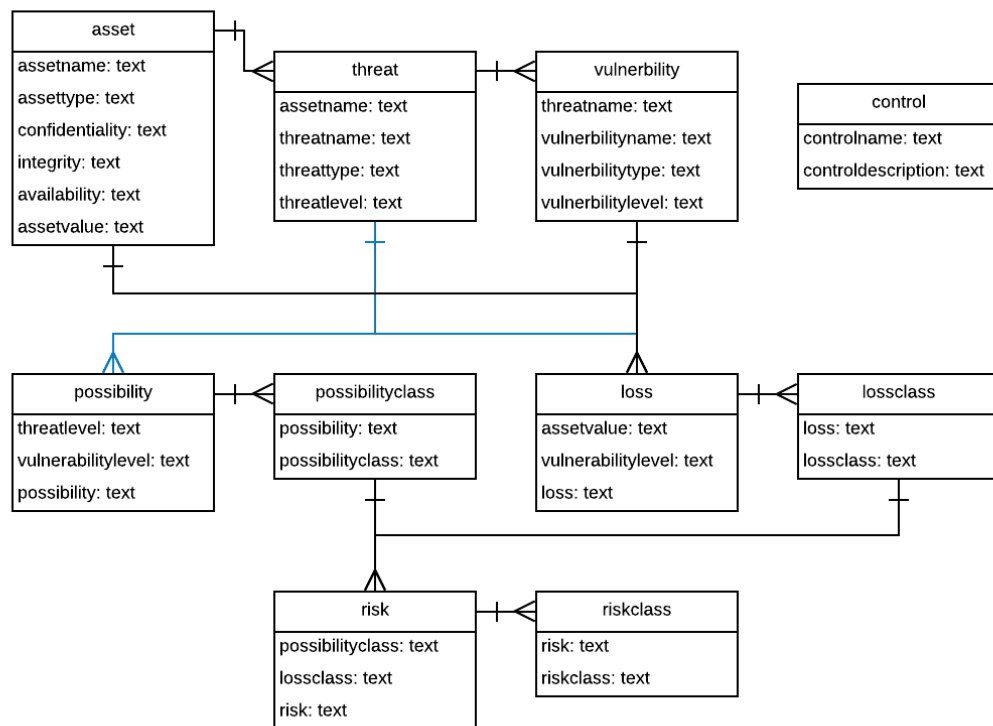


Figure 7: Information Resources Security Management Platform - database schema

System database is the base of implementation of all the operations related to data. Based on the module and functionality design, three major tables are needed for each project: asset, threat, and vulnerability. For asset table, it includes attributes (columns): asset name, asset type, confidentiality, integrity, and availability. For threat table, it includes attributes (columns): associated asset's name, threat name, threat type, and threat level. For vulnerability table, it includes attributes (columns): associated threat's name, vulnerability name, vulnerability type, and vulnerability level. As for control table, it has control name and description columns. Based on vulnerability level and threat level, the Information Resources Security Management Platform follows the metrics (explained in section 3.3), queries the pre-implemented "risk assessment" database to generate "possibility value" and "possibility class", then writes them into corresponding tables. Similarly, based on vulnerability level and asset value, the Information Resources Security Management Platform follows the metrics (explained in section 3.3), queries the pre-implemented "risk assessment" database to generate "loss value" and "loss class", then writes them into corresponding tables. Then based on "possibility class" and "loss class", it queries again to check "risk value" and "risk class", then writes it into "risk" and "riskclass" tables.

3.2 User Interface Design

This section focuses on presenting the digital prototyping and designing the user interface. Based on the module design introduced in section 3.1.1, the user interface follows the flow of the modules. As shown on the left in Figure 8, analyst is asked to log in first. Then the main page on the right in Figure 8, it shows an overall project information on the homepage of the Information Resources Security Management Platform so the analyst can add, delete, or select an existing project.

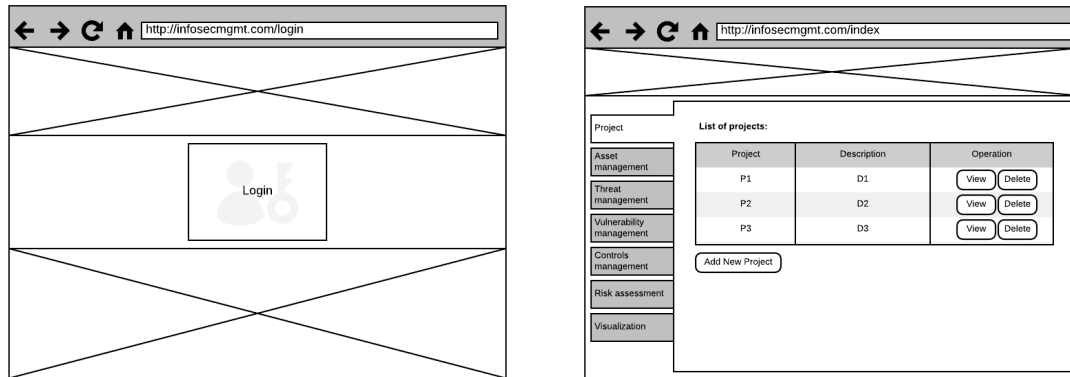


Figure 8: User login interface (left) and project management interface (right)

Then it jumps to “Asset Management” page as shown on the left in Figure 9, it lists all existing assets and corresponding type, confidentiality, integrity, and availability values. The analyst can “Add New Asset” which jumps to another page to input information for a new asset. The next tab on the navigation bar is “Threat Management” as shown on the right in Figure 9, it has the same layout as “Asset Management” which lists all threats with the associated asset, threat type, and its level. For both asset and threat management pages, for each row in the list, the analyst can choose to delete certain asset and threat.

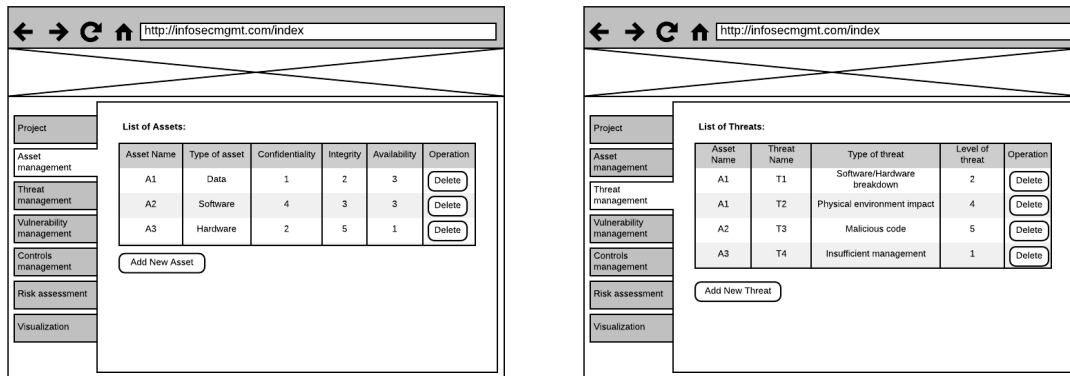


Figure 9: Asset management interface (left) and threat management interface (right)

Similar to “Asset Management” and “Threat Management” interfaces, as shown in Figure 10, the layout of the “Vulnerability Management” and “Control Management” pages

are the same, they list all existing instances and show the detailed type and level information. Additionally, the analyst has the option to add new instance or delete existing ones.

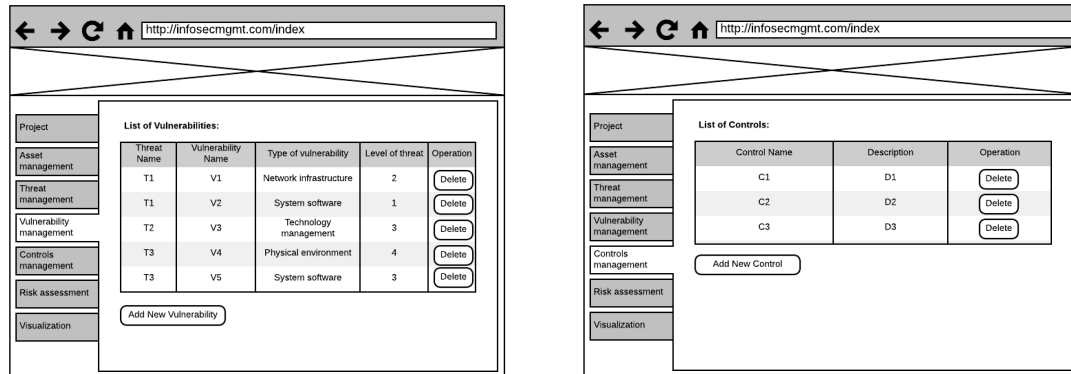


Figure 10: Vulnerability management interface (left) and control management interface (right)

The next tab in the side navigation bar is “Risk Assessment”, when the analyst chooses this tab, it automatically retrieves needed values of existing assets, threats, and vulnerabilities, then based on risk assessment metrics (explained in section 3.3), calculates the risk value and level, and lists them on the interface as shown on the left in Figure 11. On the right in Figure 11, it provides an initial prototyping of visualization. The visual graphs are built to focus on three attributes: asset, threat, and vulnerability.

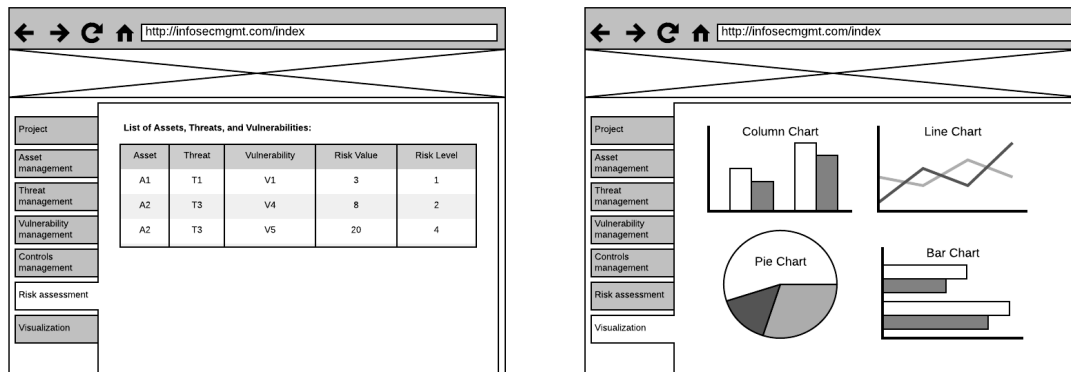


Figure 11: Risk assessment interface (left) and visualization interface (right)

3.3 Risk Assessment Metrics

Risk assessment refers to the evaluation work of quantifying possible loss to people's life, production, property... when a security accident happens, which also means a quantitative evaluation of the possibility of a security accident happens and the loss the accident might bring. For information security risk assessment, it includes the asset value of information asset, the threats it faces, and its vulnerability level, then considers all three factors to determine and evaluate the risk. To combine the three factors and evaluate the risk, Figure 12 shows the risk assessment schema:

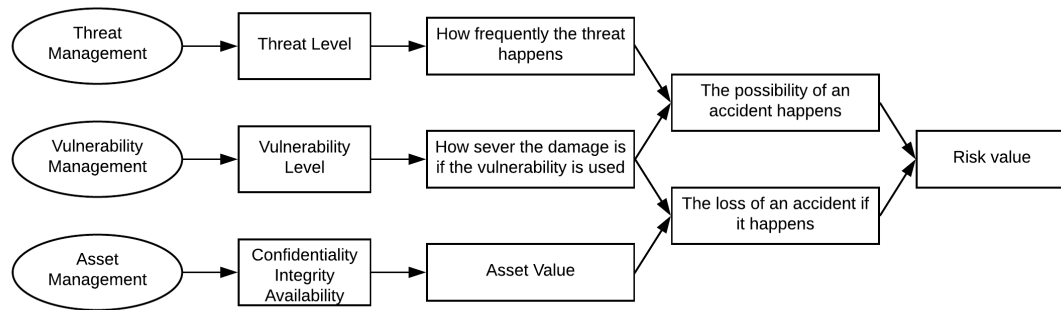


Figure 12: Risk assessment schema

The risk assessment of Information Resources Security Management Platform follows the schema in Figure 12, it extracts threat level value from the threat related table which reflects how frequently the threat happens. It also retrieves the vulnerability level value from vulnerability related table which reflects how sever the damage is if the vulnerability is used. The asset value is determined by confidentiality, integrity, and availability values by calculating the average of these three values. Each asset faces its own threat which has different levels of vulnerability. Like discussed in formal paragraph, “Risk assessment is a quantitative evaluation of the possibility of a security accident happens and the loss the accident might bring”, so how frequently the threat happens and how sever the damage is if the vulnerability is used

determine the possibility of a security accident happens, in the meanwhile, how sever the damage is if the vulnerability is used and asset value determine the loss the accident might bring. Last but not least, the possibility and the loss together decide the risk. The detailed evaluation metrics of the Information Resources Security Management Platform is explained as below:

- a. Firstly, in calculating the potential for a security accident to happen, a possibility matrix needs to be conducted, as shown in Table 5:

Vulnerability Level		1	2	3	4	5
Threat Level	1	2	4	7	11	14
	2	3	6	10	13	17
	3	5	9	12	16	20
	4	7	11	14	18	22
	5	8	12	17	20	25

Table 5: Matrix to determine the possibility value of a security accident happen

Based on the threat level and the vulnerability level, then using the possibility matrix to determine the possibility value.

Since the possibility of a security event happening needs to be included into the risk assessment calculation, in order to build the risk matrix, possibility value needs to be categorized into possibility levels, as shown in Table 6:

Possibility Value	1~5	6~11	12~16	17~21	22~25
Possibility Level	1	2	3	4	5

Table 6: Matrix to determine the possibility level of a security accident happen

- b. Secondly, in calculating the severity of a security accident, a loss matrix needs to be conducted, as shown in Table 7:

Vulnerability Level		1	2	3	4	5
Asset Value	1	2	4	7	11	14
	2	3	6	10	13	17
	3	5	9	12	16	20
	4	7	11	14	18	22
	5	8	12	17	20	25

Table 7: Matrix to determine the loss value of a security accident

Based on the asset value and the vulnerability level, then using the loss matrix to determine the loss value.

Since the loss related to a security event happening needs to be included into risk assessment calculation, in order to build the risk matrix, loss value needs to be categorized into a loss level, as shown in Table 8:

Loss Value	1~5	6~11	12~16	17~21	22~25
Loss Level	1	2	3	4	5

Table 8: Matrix to determine the loss level of a security accident

- c. Finally, in calculating the risk value, a risk matrix needs to be conducted, as shown in Table 9:

Possibility Level		1	2	3	4	5
Loss Level	1	2	4	7	11	14
	2	3	6	10	13	17
	3	5	9	12	16	20
	4	7	11	14	18	22
	5	8	12	17	20	25

Table 9: Matrix to determine the risk value of given asset, threat, and vulnerability

Based on the possibility level and the loss level, then using the risk matrix to determine the risk value, which is then used to determine the risk level, as shown in Table 10:

Risk Value	1~5	6~11	12~16	17~21	22~25
Risk Level	1	2	3	4	5

Table 10: Matrix to determine the risk level of given asset, threat, and vulnerability

This chapter thoroughly illustrates the design process and outcome of the Information Resources Security Management Platform. It starts with the overall infrastructure design, then the database schema description, user interface design, and risk assessment metrics explanation. They provide support to the development phase of the Information Resources Security Management Platform. For the outcome and detailed implementation process of the platform, please refer to Appendix A.

4 Evaluation of the Information Resources Security Management Platform in Higher Education

To evaluate the platform, I conducted four short, unstructured, informal, feedback-oriented interviews with four IT professionals that either works in IT Service in a higher education or IT department of an enterprise. The reason why I chose to interview these people is 1) they are the potential users of the platform, so their feedback and feelings are extremely valuable when assessing the feasibility and functionality of the platform. 2) they either have IT related experience in an academic setting or working experience in industry with a concentration in IT Security, so they know what will be practical and helpful to their daily work.

Each interview lasted 10 - 15 minutes. The goal of the interviews was gathering direct and immediate comments, feelings, and feedback, rather than conducting a user study to improve user experience. I expected to gain more constructive ideas and advice on the concepts and functions of the platform. These are the steps that I followed for the interviews: 1) explaining the purpose of the interview. 2) introducing the motivation and objective of the master project. 3) asking the interviewee to briefly interact with the platform. 4) further adding more explanations and demonstrations when necessary. 5) asking for their initial thoughts on what is helpful and practical as well as what can be improved and how I can improve it.

During the interview, I took notes on participants' comments and feedback. I also asked the question to the IT specialists: what are potential enhancements for future development and improvement of the project? I selected some major points from their interviews and compiled them in Table 11 below:

Role	Comment	Potential Enhancement
IT staff (centralized IT Service)	<p>“It is a very useful tool for managing information security. How can you make sure every type of asset is covered by the system?”</p> <p>The staff who are going to use this platform require solid knowledge of InfoSec to select the correct type, value, etc. How would you expect users who don’t have enough knowledge and experience to use it?”</p>	<p>Before putting the system into use, you would want to conduct more interviews and studies to make sure you have covered every possible scenario.</p> <p>Necessary training should be offered to staff so that they will gain the knowledge and technique needed to interact with the system.</p>
IT staff (branch IT Service)	<p>“There are already many existing systems in the university. Adding another one would add a lot more work. Is there any way to integrate the platform into the existing systems?”</p> <p>We are a branch of the university IT Service. How would the system work if there are different security projects in different divisions of the university?”</p>	<p>Seek opportunities to integrate the platform into existing workflow, so that adoption can be easier and more cost-efficient. Customization and consideration of how to distribute and manage sub-tasks, and their relation to the overall task will make the platform more practical.</p>
IT staff (IT service of another higher education)	<p>“It definitely can be used in my university and for my work, but individual and targeted research would need to be conducted to focus the project on threats the university faces. Also, the university probably would prefer to adopt a more wide-used and mature system. One thing you probably want to consider is that what makes your platform useful and beneficial to IT staffs work?”</p>	<p>To expand and adapt the platform to more universities, more in-depth research needs to be done.</p> <p>Moreover, making the benefits and uniqueness clearer is essential for the promotion and generalization of the system.</p>
IT Security staff (enterprise IT department)	<p>“The framework and idea behind this platform can be transferred to an enterprise setting. But there are a lot more things that need to be re-evaluated and re-considered. The enterprise version would be more complicated and would require more features and security implementations.”</p>	<p>Applying the system to enterprise still has a long way to go due to the nature of different settings, scenarios, environment, requirements, etc.</p>

Table 11: IT specialists’ comment and potential enhancement

The commenters’ views are extremely valuable since they are the potential direct users of the proposed platform. Their responses to the prompt questions revealed the additional places for future improvement, as summarized in Table 11. They all shared their ideas from their unique perspective due to their diverse background and position. The staff working in higher education raised their concerns on knowledge of the system usage and collaboration

under the fact of centralized IT and its branches. Additionally, an IT staff from another university cares more why they should adopt the system and how they can make it beneficial. While for the IT security staff in an enterprise, the platform is far from mature enough to be applied.

5 Conclusion

The paper achieves its objective of designing and developing a web-based platform to manage assets, threats, and vulnerabilities of information resources in higher education. It also provides the function of risk assessment which includes the metrics it follows and calculation it conducts. Additionally, based on the users' input, it generates visualizations to provide the user an approach to analyze and manage security projects from a visual perspective.

To answer RQ1, I conclude 6 types of asset (Data, Software, Hardware, Service, Personnel, and Others), 9 types of security threat (Software and hardware failures, Physical environment influence, Inaction or operation error, Lack of management, Malicious code, Unauthorized or abuse, Network attack, Physical attack, and Denial), and 7 types of vulnerability (Physical environment, Network infrastructure, System software, System middleware, Application system, Technical management, and Organization and management). To answer RQ2, I take the asset, threat, and vulnerability attributes into consideration and then follows the risk assessment metrics described in section 3.3 to realize the evaluation. To answer RQ3, research is conducted and there are host/server monitoring, internal/external monitoring, port activity, attack patterns, and routing behavior security visualization tools available for higher education to adopt from. To answer RQ4, chapter 3 illustrates the detailed design process and Appendix A describes how each design is implemented.

I have learned many lessons from this master project experience. These are the major ones: **1) a feasible goal and detailed plan is half of the success.** There were many ideas in my mind when I was trying to pick a topic for my master project/paper. After doing

preliminary research and discussing with my proposal class instructor, as well as my master paper advisor, apparently, not all of the ideas can be realized and implemented for a master paper. Also, having a well-planned timeline is important in terms of time and process management. At the beginning of the master paper proposal class, I took my instructor's suggestion and narrowed down the scope of the project. During the design cycle of the project, after communication with my advisor, I expanded and refined the techniques I would use for the project. Though these steps are made far from the final implementation of the product, they decide the end point that will be reached and the direction the project will go, which is half of the overall success. **2) always think about what users need.** I first thought I could design and develop anything based on my imagination since this is a project-based paper, but, obviously, the output of the project should be a system, platform, or application that can be put into the practical world, which involves the target audience of the product. This platform is designed for IT Security staff in higher education, allowing them to manage information resources security. In order to achieve that, targeted research on each aspect needed to be conducted. Moreover, gaining perspective and expectations of potential users was essential since their input helped me decide which functions were included and how they were realized and implemented. The classes I have taken in SILS such as Research Method Overview and User Interface Design helped me to conduct more effective research and in-depth analysis. **3) design and development are circular.** Everything starts with simple scratches, then develops into digital prototypes, and then into a draft product prototype. But designing and refining the design should not be a one-time action, instead, it will cycle as development happens. That is how self-reflection and other's feedback are taken into consideration for ongoing design and development. My project experience in SILS really helped me a lot during the master project. System Analysis class taught me how to conduct early-stage system analysis

and understand user's need. Visual Analytics class provided an opportunity to experience the full-stack design and development cycle and made me realize that the process is circular and how I should adjust my goals and actions based on the requirement and current state.

For the further improvement of this platform. These are several possible developments:

1) integration into existing systems. The proposed platform is designed and built individually. It will be better if every higher education organization can integrate and adopt it into its own existing systems or workflows. Using multiple systems for IT staff can be challenging when it comes to consistency and maintenance. Also, the generalization and transferability of the platform can be challenging since every higher education organization has its own relatively mature IT infrastructure. Adopting parts or an alternative version of the proposed platform would be a better option. **2) hierarchical collaboration and customization.** As described in the evaluation section, users from different levels and branches of the organization may focus on different scopes and operations when using the platform to manage information resources security. The currently proposed system treats all levels of staff equally and there is no customization available. However, in the real world, centralized IT management is as common as its branches, so the need and requirement of various features and access controls are valid concerns and focuses for the next step of design and development. **3) interactive visualizations.** The visualization module in the current proposal is not interactive, instead, it simply retrieves users' input data and displays it. To make it more dynamic and responsive based on users' interaction and need in data selection, more D3 library methods should be added to make it real-time interactive, so that users have the ability to filter and highlight the population they care about to make assessment and analysis more effective and efficient for the user.

References

- Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*, 22(4), 308-313.
- Bernstein (1998). *Against the gods: The remarkable story of risk*. New York, NY: John Wiley & Sons.
- Bishop, M. (2003). What is computer security? *IEEE Security & Privacy*, 99(1), 67-69.
- Cheung, S. K. (2014). Information Security Management for Higher Education Institutions. In *Intelligent Data analysis and its Applications*, Volume I (pp. 11-19). Springer, Cham. Retrieved from: https://link-springer-com.libproxy.lib.unc.edu/content/pdf/10.1007%2F978-3-319-07776-5_2.pdf
- Columbia University Information Security Charter. Retrieved from: http://policylibrary.columbia.edu/files/policylib/imce_shared/Information_Security_Charter.pdf
- Cortez, R. B. (September, 2017). Millions of .Edu Email Credentials Are for Sale on the Dark Web. Retrieved from: <https://edtechmagazine.com/higher/article/2017/09/millions-edu-email-credentials-are-sale-dark-web>
- Erbacher, R. F., Walker, K. L., & Frincke, D. A. (2002). Intrusion and misuse detection in large-scale systems. *IEEE Computer Graphics and Applications*, 22(1), 38-47. Retrieved from: <http://digital.cs.usu.edu/~erbacher/publications/CGAGlyphBasedIntrusionDetection.pdf>
- Fink, G. A., Muessig, P., & North, C. (2005, October). Visual correlation of host processes and network traffic. In *Visualization for Computer Security, 2005.(VizSEC 05). IEEE Workshop on* (pp. 11-19). IEEE. Retrieved from: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.97.8249&rep=rep1&type=pdf>

- Giszcak, J., Paluzzi, D., Krause, S. (2016, August 23). Pass or fail? Data privacy and cybersecurity risks in higher education. Retrieved from:
<https://www.beazley.com/documents/Insights/201606-data-privacy-and-cybersecurity-in-higher-education.pdf>
- Harris, C. E., & Hammargren, L. R. (2016, September 6). Higher education's vulnerability to cyber attacks. Retrieved from: <https://www.universitybusiness.com/article/0816-wisp>
- Hina, S., & Dominic, D. D. (2017, July). Need for information security policies compliance: A perspective in Higher Education Institutions. In *Research and Innovation in Information Systems* (ICRIIS), 2017 International Conference on (pp. 1-6). IEEE.
- Information resource. Retrieved from: https://en.wikipedia.org/wiki/Information_resource
- ISO, ISO 27000, Information Security Management System: Family of Standards, Joint Technical Committee, International Organization for Standardization and International Electrotechnical Commission (2005).
- ISO/IEC 27003, Information technology — Security techniques — Information security management system implementation guidance
- ISO/IEC 27004, Information technology — Security techniques — Information security management — Measurement
- ISO/IEC 27005, Information technology — Security techniques — Information security risk management
- Kenning, M. J. (2001). Security management standard - iso 17799/bs 7799. *BT Technology Journal*, 19(3), 132-136. Retrieved from: <http://www.tarrani.net/AttainingISO17799.pdf>
- Kvavik, R. B., & Voloudakis, J. (2003). Information technology security: Governance, strategy, and practice in higher education. Educause.
- Lakkaraju, K., Yurcik, W., Bearavolu, R., & Lee, A. J. (2004, October). NVisionIP: an interactive network flow visualization tool for security. In *Systems, Man and Cybernetics, 2004 IEEE International Conference on* (Vol. 3, pp. 2675-2680). IEEE. Retrieved from:

https://s3.amazonaws.com/academia.edu.documents/46443856/NVisionIP_An_interactive_network_flow_vi20160613-22544-orrml.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1506950711&Signature=HMLpyE4BbrZFbiuBFYGDmHNunto%3D&response-content-disposition=inline%3B%20filename%3DNVisionIP_an_interactive_network_flow_vi.pdf

Lundquist, A. E. (2015). Enterprise Risk Management (ERM) at US colleges and universities:

Administration processes regarding the adoption, implementation, and integration of ERM.

Western Michigan University. Retrieved from:

<http://scholarworks.wmich.edu/cgi/viewcontent.cgi?article=2183&context=dissertations>

Parker, D. B. (2002). Toward a New Framework for Information Security?. *Computer Security*

Handbook, Sixth Edition, 3-1.

Peltier, T. R. (2004). Information security policies and procedures: a practitioner's reference. CRC

Press.

Rao, A. (2009). Implementation of enterprise risk management (ERM) tools - a case study. *Academy of*

Accounting and Financial Studies Journal, 13(2).

Rasmussen, R. (2011, April 28). The College Cyber Security Tightrope: Higher Education Institutions

Face Greater Risks. Retrieved from: [http://www.securityweek.com/college-cyber-security-](http://www.securityweek.com/college-cyber-security-tightrope-higher-education-institutions-face-greater-risks)

[tightrope-higher-education-institutions-face-greater-risks](http://www.securityweek.com/college-cyber-security-tightrope-higher-education-institutions-face-greater-risks)

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory

study. *Computers & Security*, 27(7), 241-253. Retrieved from:

https://www.researchgate.net/profile/Yacine_Rezgui/publication/222652086_Information_security_awareness_in_higher_education_An_exploratory_study/links/565ed8c508ae4988a7bd80d2.pdf

Roscorla, T. (2016, May 18). 8 Cybersecurity Challenges Facing Higher Education. Retrieved from:

<http://www.centerdigitaled.com/higher-ed/8-Cybersecurity-Challenges-Facing-Higher-Education.html>

Security Data Visualization. SANS Institute. Retrieved from: <https://www.sans.org/reading-room/whitepapers/metrics/security-data-visualization-36387>

Shiravi, H., Shiravi, A., & Ghorbani, A. A. (2012). A survey of visualization systems for network security. IEEE Transactions on visualization and computer graphics, 18(8), 1313-1329.

Retrieved from: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6u007132>

Systems development life cycle. Retrieved from:

https://en.wikipedia.org/wiki/Systems_development_life_cycle

The CAUSE Current Issues Committee (1997, January 1). Current Issues for Higher Education Information Resources Management. Retrieved from:

<https://library.educause.edu/~media/files/library/1997/1/cem9712-pdf.pdf>

Thomas, L. R. (2013). Information Security in Higher Education: Threats & Response. Retrieved from: <https://www.giac.org/paper/gsec/2445/information-security-higher-education-threats-response/104246>

Trusted Computer System Evaluation Criteria (TCSEC). Retrieved from:

<https://www.cs.clemson.edu/course/cpsc420/material/Evaluation/TCSEC.pdf>

Universities UK (2013, November), Cyber security and universities: managing the risk. Retrieved from: <http://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2013/cyber-security-and-universities.pdf>

Wolff, J. (2015, October 11). Can Campus Networks Ever Be Secure? Retrieved from:

<https://www.theatlantic.com/technology/archive/2015/10/can-campus-networks-ever-be-secure/409813/>

Appendix A: Development of the Information Resources Security Management Platform in Higher Education

Appendix A is a supplementary section to give further explanation and illustration on the development and implementation of the web-based information resources security management platform. It introduces the development environment, the outcome of database implementation and all the front-end functionality implementation. This section uses screenshots of the actual product to show the views and interfaces of the web-based information resources security management platform. Along with key codes, it explains how every function is realized and how users are expected to interact with them.

I. Developing and Operating Environment

PHP version: 5.6

Development environment: PhpStorm

Database server: MySQL

Web server: Apache

Operating system: Mac OS

II. Implementation of the Database

The web-based platform uses a fixed database to store login information including ‘username’ and ‘userpassword’, as shown in Figure 13:

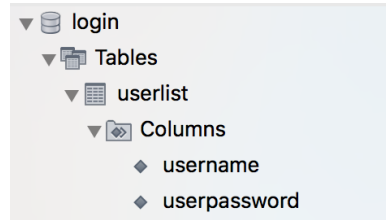


Figure 13: Login database schema

The ‘userlist’ table is used to store user name and password data, which includes the ‘username’ and ‘userpassword’ columns.

As shown in Figure 14, the ‘risk_assessment’ database stores the matrix that will be used to calculate risk value and risk level. ‘selectedProject’ is a database that stores the current database’s name that the user is working on.

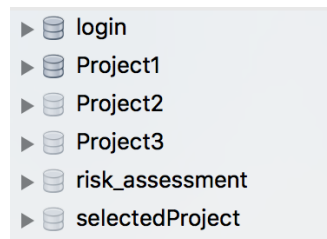


Figure 14: Databases implementation

Each project is a database and it is named by the name of the project as shown in Figure 15. For example, ‘Project1’, ‘Project2’, ‘Project3’ are testing project databases. In a project database, it contains 10 tables. ‘asset’, ‘threat’, ‘vulnerability’, ‘control’ tables that includes all the basic attributes of the project. While ‘possibility’ is determined by attributes in ‘threat’ and ‘vulnerability’ tables and ‘loss’ is determined by attributes in ‘asset’ and ‘vulnerability’ tables. Then based on possibility value and loss value, deciding the level for ‘possibilityclass’ and ‘lossclass’, which further decide the risk value and level in ‘risk’ and ‘riskclass’ tables.

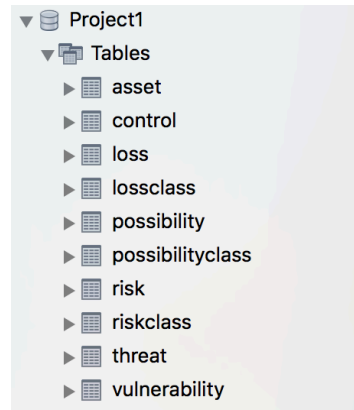


Figure 15: Project database implementation

III. Implementation of the Platform

1. Implementation of Project Management

The Project Management interface is implemented as shown in Figure 16:

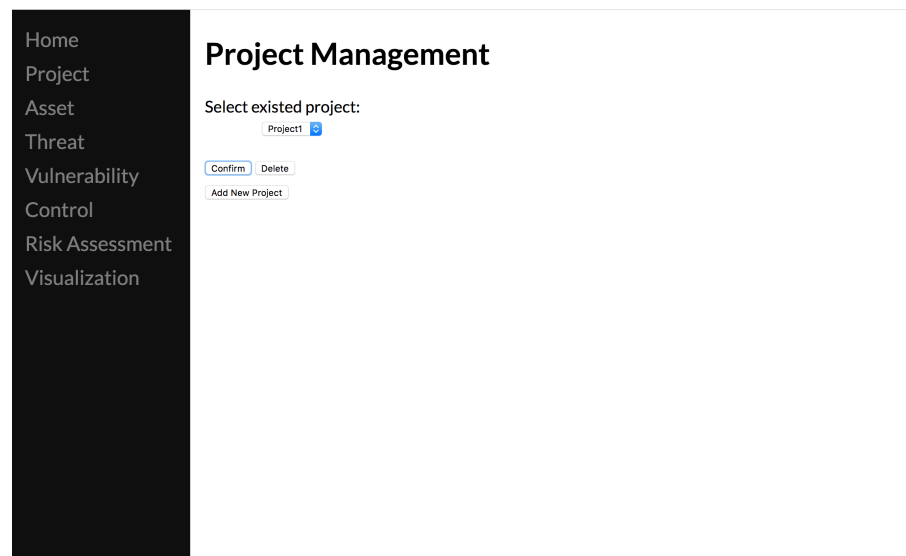


Figure 16: Project management implementation

If the project is already created and exists, then the database names are retrieved and shown in the drop-down menu. The code to implement this function is as shown below:

```
$result = mysqli_query($con, "SHOW DATABASES");
```

The code to select a project is as shown below:

```
$result = mysqli_query($con, "CREATE TABLE selectedProject"."selected (projectSelected TEXT)");
```

The code to delete a project is as shown below:

```
$result = mysqli_query($con, "DROP DATABASE ".$projectSelected);
```

If the project does not exist, the user can click on “Add New Project” button and jump to another page, as shown in Figure 17:

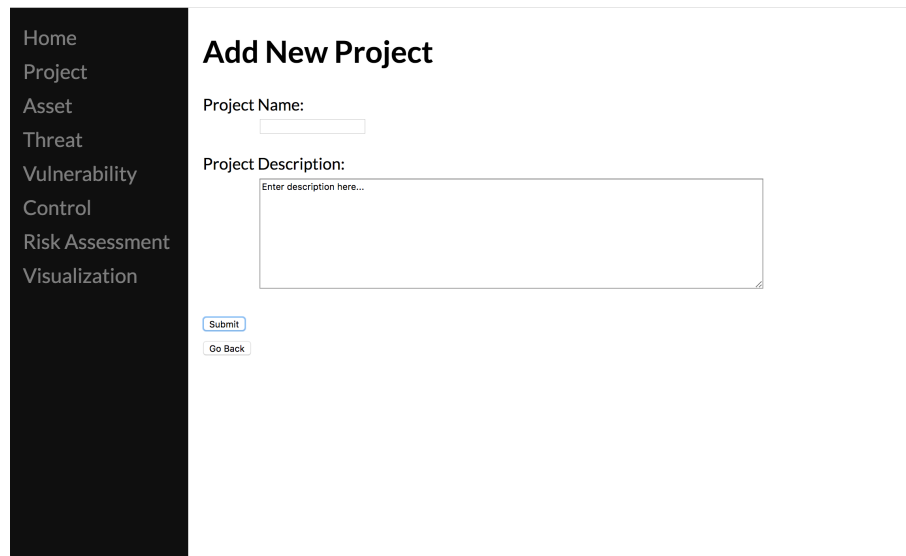


Figure 17: Add new project implementation

When a user clicks on the “Submit” button, the code to add a project is as shown below:

```
$result = mysqli_query($con, "CREATE DATABASE" .'! '.$_POST['projectName']);
```

2. Implementation of Asset Management

The Asset Management interface is implemented as shown in Figure 18:



Figure 18: Asset management implementation

If the asset is already created and exists, then the asset name, type, along with its confidentiality, integrity, and availability values are retrieved and shown in a table. The code to implement this function is as shown below:

```
$result = mysqli_query($con, "SELECT * FROM ".$result0[0].".asset");
```

The code to delete an asset is as shown below:

```
$result = mysqli_query($con, "DELETE FROM ".$result0[0].".asset WHERE assetname = '$delete_assetname'");
```

If the asset does not exist, the user can click on the “Add New Asset” button and jump to another page, as shown in Figure 19:

Home
Project
Asset
Threat
Vulnerability
Control
Risk Assessment
Visualization

Add New Asset

Asset Name:

Asset Type:

Confidentiality Value:

Value	Level	Definition
5	Very high	Contains the most important confidential information of the organization. It has a decisive influence on the fundamental interests of the organization. It will cause catastrophic damage if the information is leaked.
4	High	Contains important confidential information of the organization. It will cause serious damage to the security and the fundamental interests of the organization if the information is leaked.
3	Medium	Contains general confidential information of the organization. It will cause damage to the security and the fundamental interests of the organization if the information is leaked.
2	Low	Contains information that should only be overt to certain internal departments of the organization. It will cause slight damage to the security and the fundamental interests of the organization if the information is leaked.
1	Very low	Contains information that can be overt to the public. For example, common information processing equipment, system resources, etc.

Integrity Value:

Value	Level	Definition
5	Very high	The value of integrity is very high. Unauthorized access or modification has significant even unacceptable impact to the organization. It has great impact on business, and results in serious business interruption, which is irreparable.
4	High	The value of integrity is relatively high. Unauthorized access or modification has significant impact to the organization. It has great impact on business which is hard to repair.
3	Medium	The value of integrity is medium. Unauthorized access or modification has impact to the organization. It has obvious impact on business which is repairable.
2	Low	The value of integrity is relatively low. Unauthorized access or modification has slight impact to the organization. It has slight impact on business which is easy to repair.
1	Very low	The value of integrity is very low. Unauthorized access or modification has almost no impact to the organization. It has almost no impact on business.

Availability Value:

Value	Level	Definition
5	Very high	The value of availability is very high. The availability of information and information systems to legal users reaches to 99.9% and up per year or system is not allowed to be interrupted.
4	High	The value of availability is relatively high. The availability of information and information systems to legal users reaches to 90% and up per year or system is allowed to be interrupted no longer than 10 minutes.
3	Medium	The value of availability is medium. The availability of information and information systems to legal users reaches to 70% and up per year or system is allowed to be interrupted no longer than 30 minutes.
2	Low	The value of availability is relatively low. The availability of information and information systems to legal users reaches to 25% and up per year or system is allowed to be interrupted no longer than 60 minutes.
1	Very low	The value of availability is very low. The availability of information and information systems to legal users is lower than 25%.

Figure 19: Add new asset implementation

When a user clicks on the “Submit” button, the code to add an asset is as shown below:

```
$result = mysqli_query($con, "INSERT INTO ".$result0[0].".asset(assetname, assettype, confidentiality, integrity, availability, assetValue) VALUES ('$assetName', '$assetType', '$confidentiality', '$integrity', '$availability', '$assetvalue')");
```

3. Implementation of Threat Management

The Threat Management interface is implemented as shown in Figure 20:

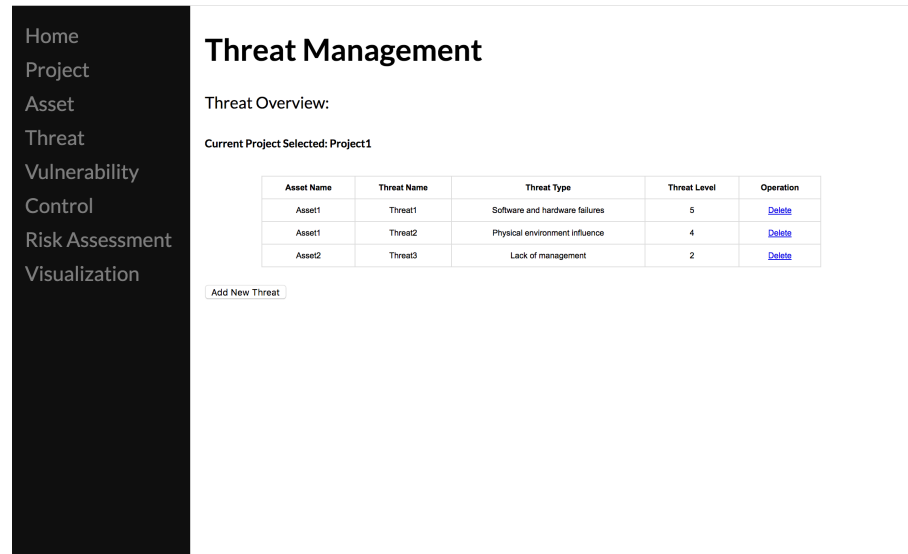


Figure 20: Threat management implementation

If the threat is already created and exists, then the threat name, type, along with its level value are retrieved and shown in a table. The code to implement this function is as shown below:

```
$result = mysqli_query($con, "SELECT * FROM ".$result0[0].".threat");
```

The code to delete a threat is as shown below:

```
$result = mysqli_query($con, "DELETE FROM ".$result0[0].".threat WHERE threatname = '$delete_threatname'");
```

If the asset does not exist, the user can click on the “Add New Threat” button and jump to another page, as shown in Figure 21:

Home
Project
Asset
Threat
Vulnerability
Control
Risk Assessment
Visualization

Add New Threat

Asset Name: Asset1

Threat Name:

Threat Type:

Threat Level:

Value	Level	Definition
5	Very high	The frequency of the occurrence is very high; or in most cases it is almost inevitable; or it can be proved that it has happened quite often.
4	High	The frequency of the occurrence is relatively high; or in most cases it is very likely to happen; or it can be proved that it has happened for several times.
3	Medium	The frequency of the occurrence is medium; or in certain cases it is likely to happen; or it can be proved that it has happened.
2	Low	The frequency of the occurrence is relatively low; or it is unlikely to happen; or it isn't proved that it has happened.
1	Very low	It is almost impossible to happen; or it has happened in a very rare and extreme case.

Figure 21: Add new threat implementation

When a user clicks on the “Submit” button, the code to add a threat is as shown below:

```
$result = mysqli_query($con, "INSERT INTO ".$result0[0].".threat(assetname, threatname, threattype, threatlevel) VALUES ('$assetName', '$threatName', '$threatType', '$threatLevel')");
```

4. Implementation of Vulnerability Management

The Vulnerability Management interface is implemented as shown in Figure 22:

Home
Project
Asset
Threat
Vulnerability
Control
Risk Assessment
Visualization

Vulnerability Management

Vulnerability Overview:

Current Project Selected: Project1

Threat Name	Vulnerability Name	Vulnerability Type	Vulnerability Level	Operation
Threat1	Vulner1	Physical environment	5	Delete
Threat1	Vulner2	Network infrastructure	4	Delete
Threat2	Vulner3	System software	3	Delete
Threat3	Vulner4	System software	1	Delete

Figure 22: Add new threat implementation

If the vulnerability is already created and exists, then the vulnerability name, type, along with its level value are retrieved and shown in a table. The code to implement this function is as shown below:

```
$result = mysqli_query($con, "SELECT * FROM ".$result0[0].".vulnerability");
```

The code to delete a threat is as shown below:

```
$result = mysqli_query($con, "DELETE FROM ".$result0[0].".vulnerability WHERE vulnerabilityname = '$delete_vulnerabilityname'");
```

If the asset does not exist, the user can click on the “Add New Vulnerability” button and jump to another page, as shown in Figure 23:

Add New Vulnerability

Threat Name: Threat1

Vulnerability Name:

Vulnerability Type: Please select

Vulnerability Level: Please select

Value	Level	Definition
5	Very high	If the threat is used, it will cause complete damage to the assets.
4	High	If the threat is used, it will cause great damage to the assets.
3	Medium	If the threat is used, it will cause general damage to the assets.
2	Low	If the threat is used, it will cause small damage to the assets.
1	Very low	If the threat is used, it will cause almost no damage to the assets.

Figure 23: Add new threat implementation

When a user clicks on the “Submit” button, the code to add a vulnerability is shown as below:

```
$result = mysqli_query($con, "INSERT INTO ".$result0[0].".vulnerability(threatname, vulnerabilityname, vulnerabilitytype, vulnerabilitylevel) VALUES ($threatName, '$vulnerabilityName', '$vulnerabilityType', '$vulnerabilityLevel')");
```

5. Implementation of Control Management

The Control Management interface is implemented as shown in Figure 24:

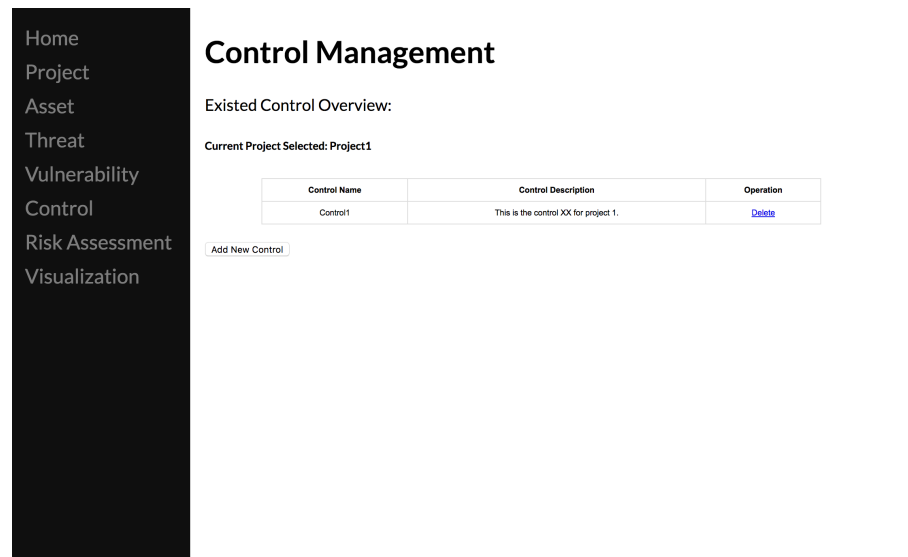


Figure 24: Control management implementation

If the control is already created and exists, then the control name along with its description are retrieved and shown in a table. The code to implement this function is as shown below:

```
$result = mysqli_query($con, "SELECT * FROM ".$result0[0].".control");
```

The code to delete a threat is as shown below:

```
$result = mysqli_query($con, "DELETE FROM ".$result0[0].".control WHERE controlname = '$delete_controlname'");
```

If the asset does not exist, the user can click on the “Add New Control” button and jump to another page, as shown in Figure 25:

Figure 25: Add new control implementation

When a user clicks on the “Submit” button, the code to add a control is as shown below:

```
$result = mysqli_query($con, "INSERT INTO ".$result0[0].".control(controlName, controlDescription) VALUES ('$controlName','$controlDescription')");
```

6. Implementation of Risk Assessment

The Risk Assessment interface is implemented as shown in Figure 26:

Asset	Threat	Vulnerability	Risk Value	Risk Level
Asset1	Threat1	Vulner1	25	5
Asset1	Threat1	Vulner2	23	4
Asset1	Threat2	Vulner3	16	3
Asset2	Threat3	Vulner4	3	1

Figure 26: Risk assessment implementation

If the asset, threat, and vulnerability information are already created and exist, then the risk value and level are calculated and shown in a table. The code to implement this function is as shown below:

```
$risk = mysqli_query($con, "SELECT risk FROM ".$risk_assessment.".risk WHERE lossclass = '$result_lossclass[0]' and possibilityclass = '$result_possibilityclass[0]'");

$riskclass = mysqli_query($con, "SELECT riskclass FROM ".$risk_assessment.".riskclass WHERE risk = '$result_risk[0]'");
```

7. Implementation of Visualization

The Visualization interface is implemented as shown in Figure 27:

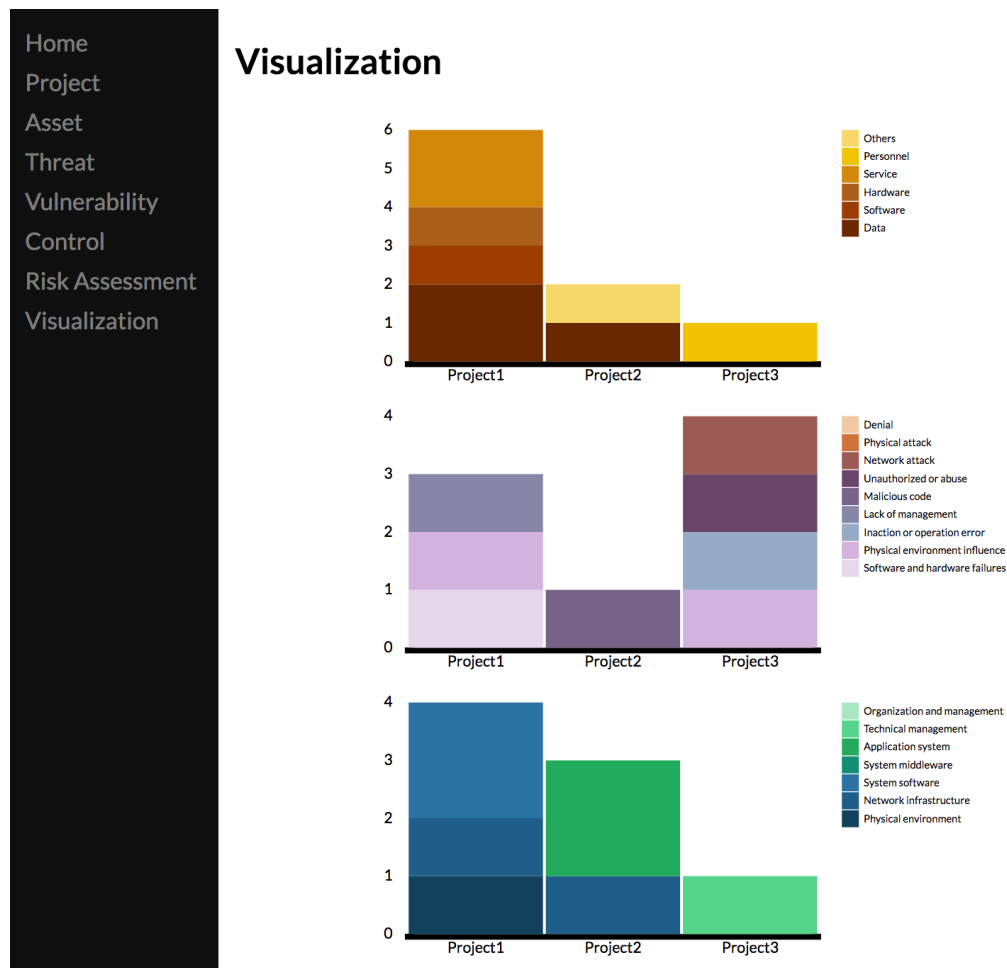


Figure 27: Visualization implementation

The three graphs are generated based on all projects that have been created and exist in the database. They are for asset overview, threat overview, and vulnerability overview. I use PHP for data retrieval and formatting, then use the JavaScript D3 library to take the datasets in and then generate three stacked bar charts, which provide the user a visual method to analyze, assess, and manage all the security projects from different concentrations. I used different color schemas to differentiate the three attributes. The legends on the right show all the types of each attribute. If the user hovers over a stacked bar, it will show a tool tip that is the number of that specific type of attribute in the project. For example, hovering over the Green bar in project 2 in the bottom of the 3 bar graphs would show 2. Hovering over the blue below it would show 1.